CLAIMS:

1. (Currently Amended): A method, in a data processing system, for handling personally identifiable information, said method comprising:

providing, in a computer, a first set of object classes representing active entities in an information-handling process, wherein a limited number of privacy-related actions represent operations performed on data and wherein each of the active entities is a human being or legal entity;

providing, in said computer, a second set of object classes representing data and rules in said information-handling process, wherein at least one object class has said rules associated with said data, and wherein said data represents said personally identifiable information; and

processing transactions, in the data processing system, involving said personally identifiable information, using said computer and said first and second set of object classes, so as to enforce a privacy policy, associated with the personally identifiable information and defined by said rules, against one or more active entities represented by said first set of object classes, wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity, wherein:

a first active entity represented by a first object class in said first set of object classes is a first data user that requests said personally identifiable information from a data subject that is a second active entity represented by a second object class in said first set of object classes,

said data subject is an active entity that is personally identifiable by said personally identifiable information;

a third active entity represented by a third object class in said first set of object classes is a second data user that requests personally identifiable information from said first data user, and

said rules define if and how said personally identifiable information may be provided, by said first data user, to said second data user.

2. (Previously Presented): The method of claim 1, wherein said first set of object classes include one or more object classes representing parties, selected from the group consisting of

a data user object class,

a data subject object class,

a guardian object class, and

a privacy authority object class.

3. (Previously Presented): The method of claim 1, wherein said at least one object class, having said rules associated with said data, represents a filled paper form, including both collected data and rules regarding said collected data.

4. (Previously Presented): A method, in a data processing system, for improving the handling of personally identifiable information, said method comprising:

performing, in the data processing system, an initial assessment of an information-handling process;

constructing, in said data processing system, a model of said information-handling process, based on said initial assessment; and

providing output, from said data processing system, based on said initial assessment and constructing, that identifies at least one way in which said personally identifiable information could be better handled;

wherein said constructing includes:

representing entities, data, and rules in said information–handling process by using a limited number of object classes;

representing operations performed on data by using a limited number of privacy-related actions; and

representing transactions by using said limited number of object classes and said limited number of privacy-related actions.

5. (Original): The method of claim 4, wherein said providing output further comprises identifying at least one way in which said information-handling process could be improved.

6. (Original): The method of claim 4, wherein said providing output further comprises identifying at least one way to improve compliance with a law or contract.

7. (Original): The method of claim 4, further comprising enforcing compliance with a law or contract.

8. (Original): The method of claim 4, further comprising designing a modification to said information-handling process, based on said constructing and providing.

9. (Original): The method of claim 8, wherein said designing a modification further comprises designing a modification to improve compliance with a law or contract governing said information handling process.

10. (Original): The method of claim 4, wherein said limited number of object classes includes one or more object classes representing parties selected from the group consisting of

a data user object class,
a data subject object class,
a guardian object class, and
a privacy authority object class.

11. (Original): The method of claim 4, wherein said limited number of object classes include at least one object class wherein rules are associated with data.

12. (Currently Amended): A system for handling personally identifiable information, said system comprising:

means for providing, in a computer, a first set of object classes representing active entities in an information-handling process, wherein a limited number of privacy-related actions represent operations performed on data and wherein each of the active entities is a human being or legal entity;

means for providing, in said computer, a second set of object classes representing data and rules in said information-handling process, wherein at least one object class has said rules associated with said data, and wherein said data represents said personally identifiable information; and

means for processing transactions, in a data processing system, involving said personally identifiable information, using said computer and said first and second set of object classes, so as to enforce a privacy policy, associated with the personally identifiable information and defined by said rules, against one or more active entities represented by said first set of object classes, wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity, wherein:

a first active entity represented by a first object class in said first set of object classes is a first data user that requests said personally identifiable information from a data subject that is a second active entity represented by a second object class in said first set of object classes,

said data subject is an active entity that is personally identifiable by said personally identifiable information;

a third active entity represented by a third object class in said first set of object classes is a second data user that requests personally identifiable information from said first data user, and

said rules define if and how said personally identifiable information may be provided, by said first data user, to said second data user.

13. (Previously Presented): The system of claim 12, wherein said first set of object classes include one or more object classes selected from the group consisting of

a data user object class,

a data subject object class,

a guardian object class, and

a privacy authority object class.

14. (Previously Presented): The system of claim 12, wherein said at least one object class, having said rules associated with said data, represents a filled paper form, including both collected data and rules regarding said collected data.

15. (Currently Amended): A computer-usable medium having computer-executable instructions for handling personally identifiable information, said computer executable instructions comprising:

means for providing in a computer a first set of object classes representing active entities in an information-handling process, wherein a limited number of privacy-related actions represent operations performed on data and wherein each of the active entities is a human being or legal entity;

means for providing in said computer a second set of object classes representing data and rules in said information-handling process, wherein at least one object class has said rules associated with said data, and wherein said data represents said personally identifiable information; and

means for processing transactions, in a data processing system, involving said personally identifiable information, using said computer and said first and second set of object classes, so as to enforce a privacy policy, associated with the personally identifiable information and defined by said rules, against one or more active entities represented by said first set of object classes, wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity, wherein:

a first active entity represented by a first object class in said first set of object classes is a first data user that requests said personally identifiable information from a data subject that is a second active entity represented by a second object class in said first set of object classes,

said data subject is an active entity that is personally identifiable by said personally identifiable information;

a third active entity represented by a third object class in said first set of object classes is a second data user that requests personally identifiable information from said first data user, and

said rules define if and how said personally identifiable information may be provided, by said first data user, to said second data user.

16. (Previously Presented): The computer-usable medium of claim 15, wherein said first set of object classes include one or more object classes representing parties, selected from the group consisting of

a data user object class,

a data subject object class,

a guardian object class, and

a privacy authority object class.

17. (Previously Presented): The computer-usable medium of claim 15, wherein said at least one object class, having said rules associated with said data, represents a filled paper form, including both collected data and rules regarding said collected data.

18. (Canceled)

19. (Currently Amended): The method of claim [[18]] 1, further comprising:

transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user.

20. (Canceled)

21. (New): The system of claim 12, further comprising:

means for transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user.

22. (New): The computer-usable medium of claim 15, said computer executable instructions further comprising:

means for transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user.